تنفيذ شبكة VPN المستندة إلى المسار من موقع إلى موقع IKEv2 على موجهات Cisco باستخدام IPv6

المحتويات

المقدمة

يصف هذا المستند تكوين إعداد نفق IPv6، مستند إلى المسار، من موقع إلى موقع بين موجهات Cisco باستخدام بروتوكول تبادل مفتاح الإنترنت الإصدار 2 (IKEv2).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بتكوين واجهة سطر الأوامر Cisco IOS®/Cisco IOS® XE
- معرفة أساسية ببروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP) وبروتوكولات IPsec
- فهم عنونة IPv6 والتوجيه

المكونات المستخدمة

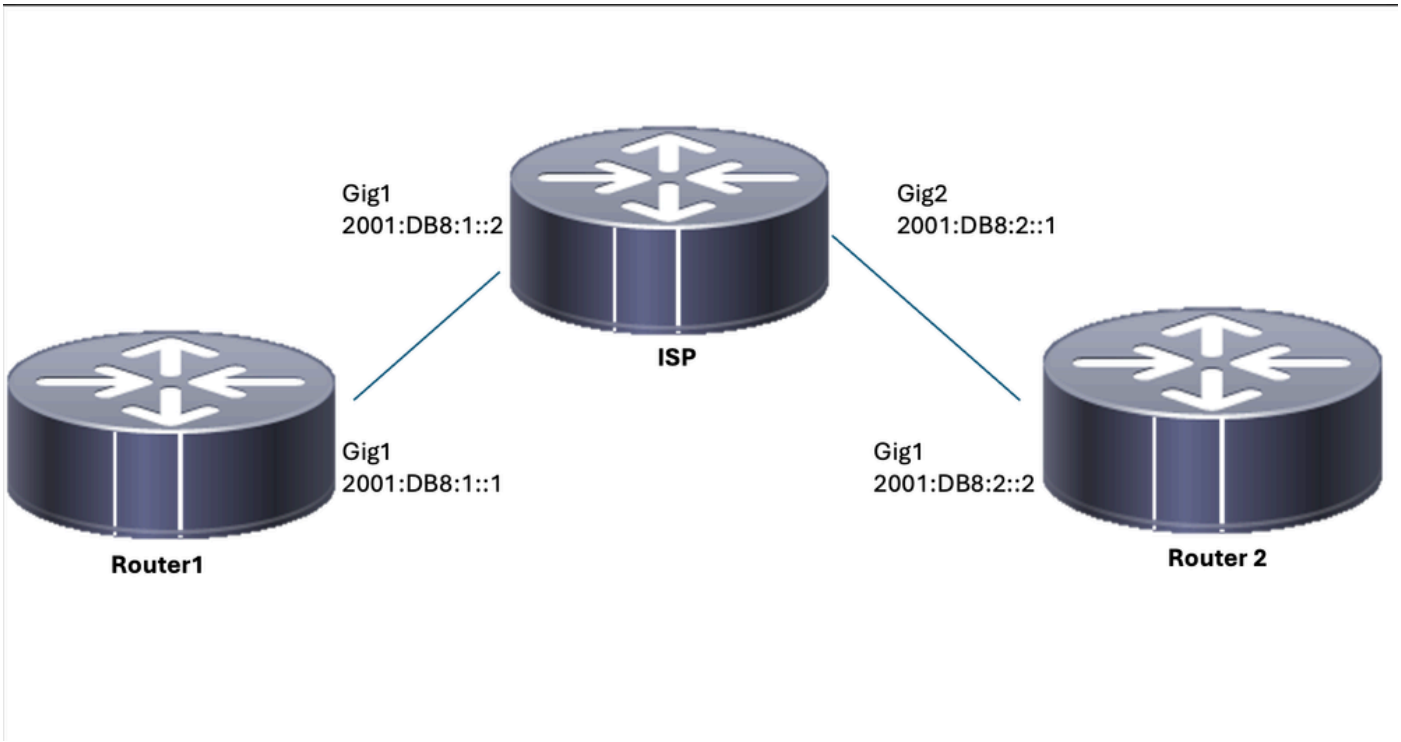
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- IOS XE من Cisco يشغل 17.03.04a كموجه محلي
- برنامج IOS الذي يشغل 17.03.04a كموجه عن بعد من Cisco

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الرسم التخطيطي للشبكة



تكوينات الموجه المحلي

الخطوة 1. تمكين توجيه البث الأحادي ل IPv6.

```
ipv6 unicast-routing
```

الخطوة 2. قم بتكوين واجهات الموجه.

```
interface GigabitEthernet1
ipv6 address 2001:DB8:1::1/64
no shutdown

interface GigabitEthernet2
ipv6 address FC00::1/64
no shutdown
```

الخطوة 3. تعيين المسار الافتراضي ل IPv6.

```
ipv6 route ::/0 GigabitEthernet1
```

الخطوة 4. تكوين مقترح IKEv2.

```
crypto ikev2 proposal IKEv2-PROP
encryption aes-cbc-128
integrity sha1
group 14
```

الخطوة 5. تكوين سياسة IKEv2.

```
crypto ikev2 policy IKEv2-POLI
proposal IKEv2-PROP
```

الخطوة 6. قم بتكوين حلقة المفاتيح باستخدام مفتاح مشترك مسبقا.

```
crypto ikev2 keyring IPV6_KEY
peer Remote_IPV6
 address 2001:DB8:2::2/64
 pre-shared-key cisco123
```

الخطوة 7. قم بتكوين ملف تعريف IKEv2.

```
crypto ikev2 profile IKEV2-PROF
 match identity remote address 2001:DB8:2::2/64
 authentication remote pre-share
 authentication local pre-share
 keyring local IPV6_KEY
```

الخطوة 8. تكوين نهج المرحلة 2.

```
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
mode tunnel
```

الخطوة 9. تكوين ملف تعريف IPsec.

```
crypto ipsec profile IPSEC-PROF
 set transform-set ESP-AES-SHA
 set ikev2-profile IKEV2-PROF
```

الخطوة 10. قم بتكوين واجهة النفق.

```
interface Tunnel1
 ipv6 address 2001:DB8:3::1/64
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv6
 tunnel destination 2001:DB8:2::2
 tunnel protection ipsec profile IPSEC-PROF
end
```

الخطوة 11. قم بتكوين المسارات لحركة المرور المفيدة.

```
ipv6 route FC00::/64 2012::1
```

التكوين النهائي للموجه المحلي

```
ipv6 unicast-routing
!
interface GigabitEthernet1
ipv6 address 2001:DB8:1::1/64
no shutdown

!

interface GigabitEthernet2
ipv6 address FC00::1/64
no shutdown

!

ipv6 route ::/0 GigabitEthernet1

!

crypto ikev2 proposal IKEv2-PROP
encryption aes-cbc-128
integrity sha1
group 14
```

```
!

crypto ikev2 policy IKEv2-POLI
proposal IKEv2-PROP

!

crypto ikev2 keyring IPV6_KEY
peer Remote_IPV6
 address 2001:DB8:2::2/64
 pre-shared-key cisco123

!

crypto ikev2 profile IKEV2-PROF
 match identity remote address 2001:DB8:2::2/64
 authentication remote pre-share
 authentication local pre-share
 keyring local IPV6_KEY

!

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
mode tunnel

!

crypto ipsec profile Prof1
 set transform-set ESP-AES-SHA

 !

 crypto ipsec profile IPSEC-PROF
 set transform-set ESP-AES-SHA
 set ikev2-profile IKEV2-PROF

!

interface Tunnel1
 ipv6 address 2001:DB8:3::1/64
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv6
 tunnel destination 2001:DB8:2::2
 tunnel protection ipsec profile IPSEC-PROF
end

!

ipv6 route FC00::/64 2012::1
```

تكوين ISP

```
ipv6 unicast-routing
!
!
interface GigabitEthernet1
```

```
 description Link to R1
 ipv6 address 2001:DB8:1::2/64
!
interface GigabitEthernet2
 description Link to R3
 ipv6 address 2001:DB8:2::1/64
!
!
!
ipv6 route 2001:DB8:1::/64 GigabitEthernet1
ipv6 route 2001:DB8:2::/64 GigabitEthernet2
!
```

التكوين النهائي للموجه عن بعد

```
ipv6 unicast-routing
!
interface GigabitEthernet1
ipv6 address 2001:DB8:2::2/64
no shutdown

!

interface GigabitEthernet2
ipv6 address FC00::2/64
no shutdown

!

ipv6 route ::/0 GigabitEthernet1

!

crypto ikev2 proposal IKEv2-PROP
encryption aes-cbc-128
integrity sha1
group 14

!

crypto ikev2 policy IKEv2-POLI
proposal IKEv2-PROP

!

crypto ikev2 keyring IPV6_KEY
peer Remote_IPV6
 address 2001:DB8:1::1/64
 pre-shared-key cisco123

!

crypto ikev2 profile IKEV2-PROF
 match identity remote address 2001:DB8:1::1/64
 authentication remote pre-share
 authentication local pre-share
 keyring local IPV6_KEY
```

```
!

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
mode tunnel

!

crypto ipsec profile Prof1
 set transform-set ESP-AES-SHA

 !

 crypto ipsec profile IPSEC-PROF
 set transform-set ESP-AES-SHA
 set ikev2-profile IKEV2-PROF

!

interface Tunnel1
 ipv6 address 2001:DB8:3::2/64
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv6
 tunnel destination 2001:DB8:1::1
 tunnel protection ipsec profile IPSEC-PROF
end

!

ipv6 route FC00::/64 2012::1
```

التحقق

```
On Router 1

R1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
2           none/none             READY
Local  2001:DB8:1::1/500
Remote  2001:DB8:2::2/500
      Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: P
      Life/Active Time: 86400/75989 sec

R1#show crypto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 2001:DB8:1::1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (::/0/0/0)
   remote ident (addr/mask/prot/port): (::/0/0/0)
   current_peer 2001:DB8:2::2 port 500
     PERMIT, flags={origin_is_acl,}
```

```
    #pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 2001:DB8:1::1,
     remote crypto endpt.: 2001:DB8:2::2
     plaintext mtu 1422, path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb GigabitEthernet1
     current outbound spi: 0x9DC2A6F6(2646779638)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x18569EF7(408329975)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2104, flow_id: CSR:104, sibling_flags FFFFFFFF80000049, crypto map: Tunnel1-head-0
         sa timing: remaining key lifetime (k/sec): (4608000/1193)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x9DC2A6F6(2646779638)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2103, flow_id: CSR:103, sibling_flags FFFFFFFF80000049, crypto map: Tunnel1-head-0
         sa timing: remaining key lifetime (k/sec): (4608000/1193)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:


On Router 2

R2#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
1          none/none             READY
Local  2001:DB8:2::2/500
Remote  2001:DB8:1::1/500
      Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: P
      Life/Active Time: 86400/19 sec

R2#show cryto ipsec sa

interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 2001:DB8:2::2

   protected vrf: (none)
```

```
local  ident (addr/mask/prot/port): (::/0/0/0)
remote ident (addr/mask/prot/port): (::/0/0/0)
current_peer 2001:DB8:1::1 port 500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 14, #pkts encrypt: 14, #pkts digest: 14
 #pkts decaps: 14, #pkts decrypt: 14, #pkts verify: 14
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0

  local crypto endpt.: 2001:DB8:2::2,
  remote crypto endpt.: 2001:DB8:1::1
  plaintext mtu 1422, path mtu 1500, ipv6 mtu 1500, ipv6 mtu idb GigabitEthernet1
  current outbound spi: 0xEF1D3BA2(4011670434)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
   spi: 0x9829B86D(2552871021)
     transform: esp-aes esp-sha-hmac ,
     in use settings ={Tunnel, }
     conn id: 2006, flow_id: CSR:6, sibling_flags FFFFFFFF80000049, crypto map: Tunnel1-head-0
      sa timing: remaining key lifetime (k/sec): (4608000/3556)
     IV size: 16 bytes
     replay detection support: Y
     Status: ACTIVE(ACTIVE)

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0xEF1D3BA2(4011670434)
     transform: esp-aes esp-sha-hmac ,
     in use settings ={Tunnel, }
     conn id: 2005, flow_id: CSR:5, sibling_flags FFFFFFFF80000049, crypto map: Tunnel1-head-0
      sa timing: remaining key lifetime (k/sec): (4607998/3556)
     IV size: 16 bytes
     replay detection support: Y
     Status: ACTIVE(ACTIVE)

  outbound ah sas:

  outbound pcp sas:
```

استكشاف الأخطاء وإصلاحها

لاستكشاف أخطاء النفق وإصلاحها، أستخدم أوامر تصحيح الأخطاء التالية:

- debug crypto ikev2
- debug crypto ikev2 error
- debug crypto ipsec
- debug crypto ipsec error

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).